Stiftung Warentest

test

Digitale Welt für Einsteiger

Tracking verhindern, Daten schützen, anonym surfen, VPN nutzen

Spurlos im Internet

Inhaltsverzeichnis

Sie haben etwas zu verbergen!

Das Internet – unendliche Weiten. Und auch unendliche Mengen von Daten. Wenn Sie eine Seite aufrufen, hinterlassen Sie Spuren. Wenn Sie online etwas kaufen, geben Sie Daten ein. Wenn Sie eine E-Mail verschicken: Daten. Soziale Netzwerke? Daten, Daten, Daten. Es lohnt sich, etwas genauer hinzuschauen: Welche Daten schwirren da draußen herum und was ist deren Nutzen oder Risiko?

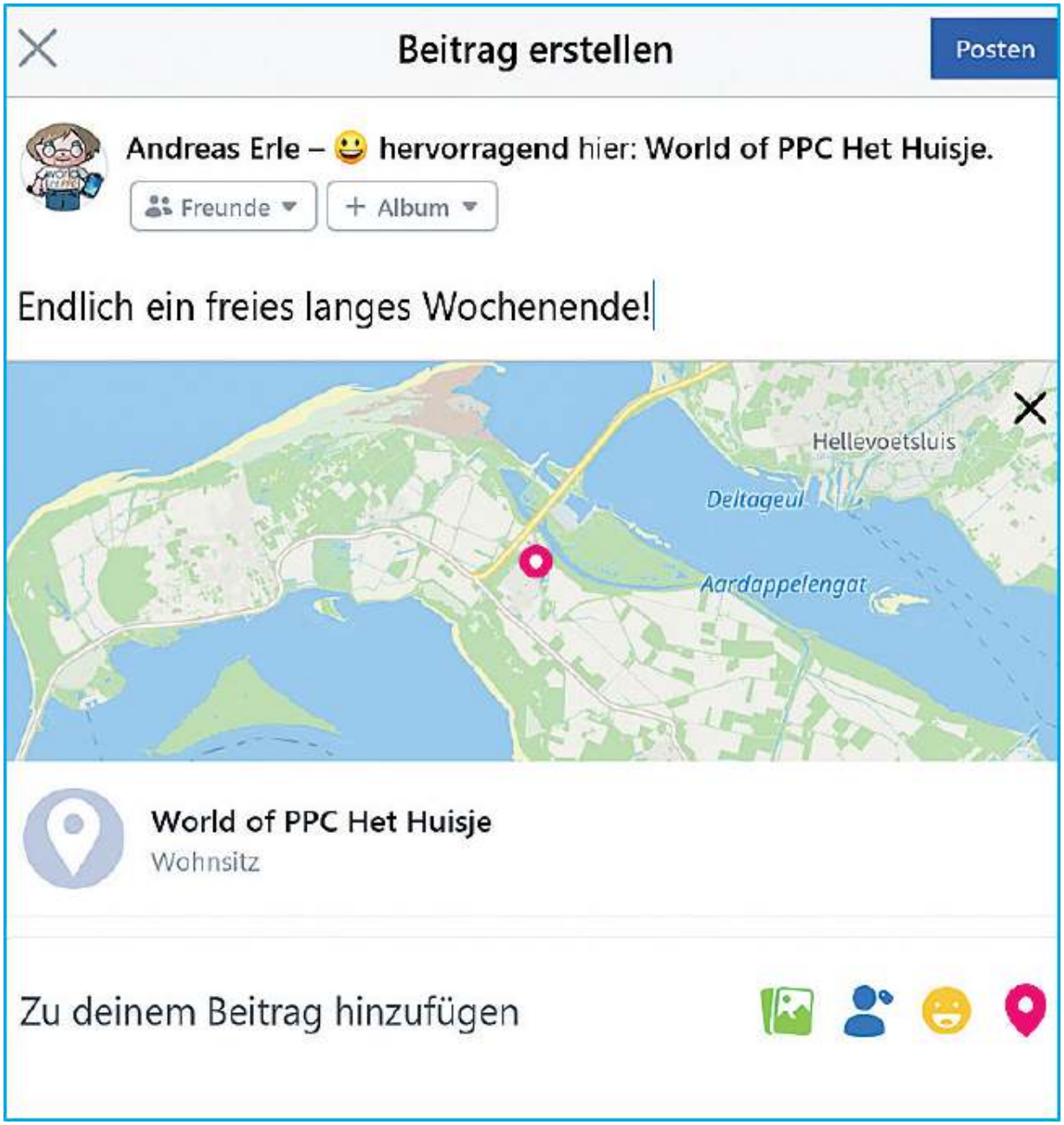
Anonymität schafft Privatsphäre

Es gibt nahezu endlos viele Geräte, die miteinander vernetzt sind. Nicht nur PC, Tablet und Smartphone, sondern auch Ihr Fernseher, der Sprachassistent, Ihre Webcam im Ferienhaus und der intelligente Rauchmelder – sie alle sammeln Informationen, oder anders genannt: Daten. Diese Geräte stehen nicht allein da, sondern sie verbinden sich. Über das Internet, im heimischen Netzwerk, durch eigene sogenannte Mesh-Netzwerke. Damit befinden sich Ihre Daten nicht nur an einem Ort, sondern wandern von Gerät zu Gerät, von Speicher zu Speicher. Eines sollten Sie dabei nicht vergessen: Diese Daten gehören Ihnen. Die klassische Aussage „Ich habe nichts zu verbergen“ nehmen viele zurück, sobald ihnen klar wird, wie viel vermeintlich harmlose Daten verraten und für welche Zwecke sie sich verwenden lassen. Sie sollten selbst entscheiden (können), wer welche Daten von Ihnen sieht und nutzt.

Chance oder Falle?

Die öffentliche Diskussion geht seit einigen Jahren deutlich in eine Richtung: Datenschutz geht vor allem anderen, wer Daten verarbeitet, ist ein potenzieller Bösewicht, und Datenlecks sind ohnehin die Schuld, ja vielleicht sogar Absicht desjenigen, der die Daten gespeichert hat. Die Unternehmen, die Ihre Daten verwenden, haben da eine ganz andere Sicht: Sie bekommen eine Dienstleistung, dafür bekommen die Unternehmen Ihre Daten. Ein

einfaches Geschäft. Wie immer liegt die Wahrheit irgendwo dazwischen.
Uns Nutzern ist eine gewissermaßen schizophrene Haltung eigen: Wenn wir etwas gut finden, dann schieben wir unsere Bedenken beiseite. Nur, um sie dann wieder hervorzuholen, wenn es uns in den Kram passt. Ein paar Beispiele gefällig?



Die sozialen Netzwerke sind ja oft ein Jahrmarkt der Eitelkeiten. Wir fühlen uns gut, wenn wir der Welt mitteilen können, dass wir gerade an einem exklusiven Ort Urlaub machen. Die Kehrseite vergessen wir gern: Jeder, der den entsprechenden Eintrag in den sozialen Netzwerken sieht, kann messerscharf schließen, dass wir nicht zu Hause sind. Optimale Voraussetzungen für einen Einbruch!
Oder die Sprachassistenten: Nicht erst seit Amazons Alexa sind Sprachassistenten in Mode. Von den ersten Diktierprogrammen bis zu Siri, Bixby und Cortana nutzen wir die Freiheit und den Komfort der Sprachbedienung, auch in dem Bewusstsein, dass diese Daten ja an irgendeiner Stelle verarbeitet und in ausführbare Befehle umgesetzt werden müssen. Eine Wanze im Smartphone ist hingegen eine Horrorvision aus einem Agententhriller, die keiner von uns möchte.
Vielleicht noch deutlicher macht es die – durchaus angemessene – Skepsis gegenüber den großen Konzernen. Google, Microsoft, Apple, Amazon und viele mehr sind so in unser Leben integriert, dass sie unvermeidbar Daten sammeln. Allein mag man das noch akzeptieren. Als Facebook 2014 aber den Messenger WhatsApp übernahm, war das Geschrei groß: Facebook noch mehr Daten in den virtuellen Hals werfen? Für viele Anwender keine Option. Auch für die nicht, die vorher schon WhatsApp und Facebook eifrig genutzt haben.
Hier wurden viele Anwender wach und einfallsreich: Weniger datenhungrige Alternativen sollten her. Für WhatsApp gab es mit Threema eine Alternative, die eine wirklich vertrauliche Kommunikation ermöglichen sollte. Erst wenn zwei Geräte sich tatsächlich einmal „gesehen hatten“, galten sie als vertrauenswürdig. Das Verfahren war einfach: Das eine Gerät zeigte auf seinem Bildschirm einen QR-Code an, das andere musste ihn scannen. Damit

war klar, dass die beiden Geräte (und damit auch deren Besitzer) sich gegenseitig begegnet sind und ihr Vertrauen ausgesprochen haben. Klingt gut, meinen Sie? Prinzipiell schon. Wenn da nicht der ein oder andere Schlaukopf auf die Idee gekommen wäre, seinen geheimen Threema-QR-Code auf Facebook zu posten, damit all seine Freunde ihn scannen konnten. Vertraulichkeit geht anders!

Anonymität als Schutz

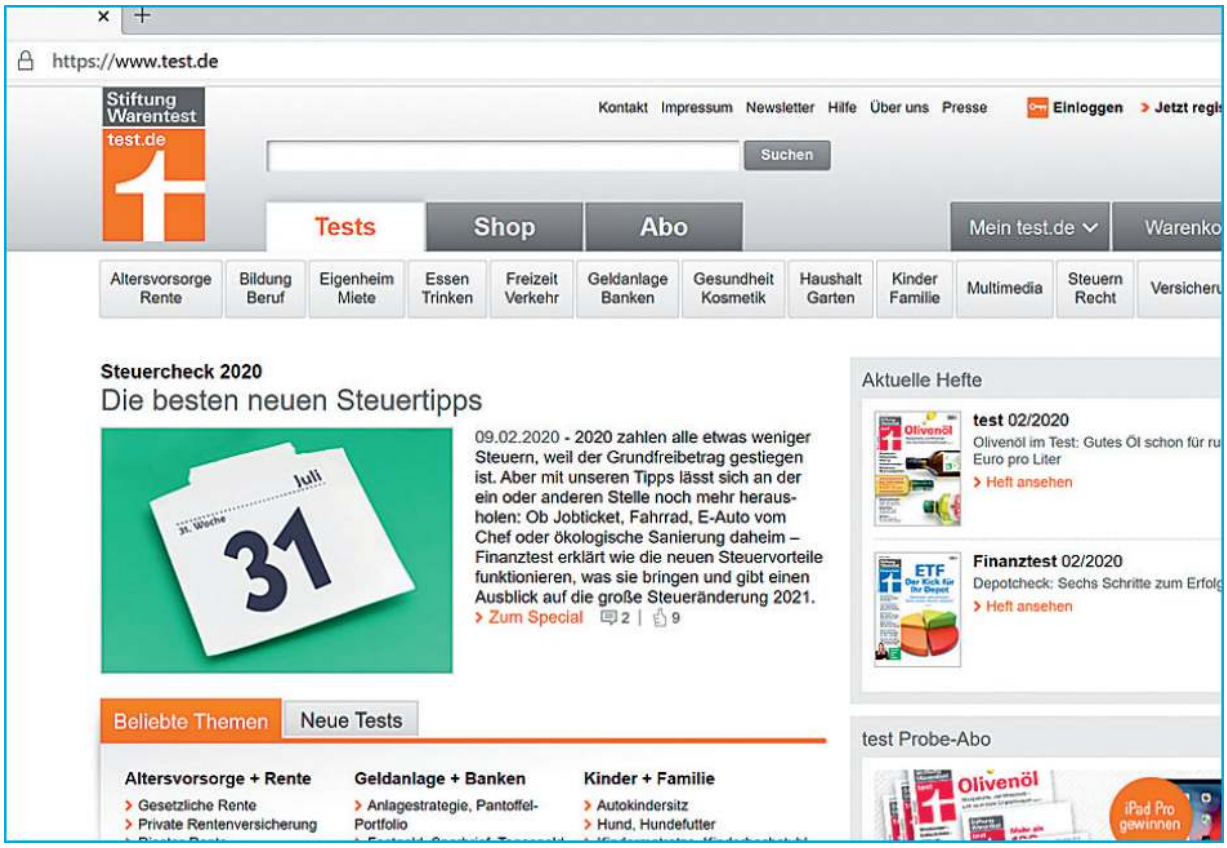
Ein immer wieder genannter Begriff in diesem Zusammenhang ist Anonymität. Wikipedia definiert diesen Begriff so:

> **Anonymität**
>
> Anonymität (von altgriechisch anónymos „ohne Namen“) bezeichnet das Fehlen der Zuordnung einer Person zu einer von ihr ausgeübten Handlung bis hin zur absichtlichen Geheimhaltung. Sie kann zum Schutz der Freiheit des Einzelnen dienen. Der Gesetzgeber hat sie deswegen in verschiedenen Bereichen vorgesehen. So werden beispielsweise das Wahlgeheimnis verpflichtend, die anonyme Information, Meinungsäußerung und Versammlung als Rechte verfassungsrechtlich garantiert.

Im Internet bedeutet Anonymität, dass das, was Sie online tun, und die Daten, die Sie dabei hinterlassen, nicht auf Sie als Person zurückgeführt werden können. Je anonymer Sie im Internet sind, desto weniger kann Ihnen passieren. Wer Sie nicht kennt, kann Ihnen nichts Böses. Damit ist es eines der wichtigsten Ziele bei der Nutzung des Internets und seiner Dienste, die Anonymität zu wahren.

Private Daten: Währung und Risiko

Wenn die vorangegangenen Ausführungen den Eindruck erweckt haben, dass die Preisgabe Ihrer Daten immer ein Risiko und das Internet deshalb „böse“ ist, dann ist das nur ein Teil der Wahrheit. Das Internet funktioniert nun mal nur mit Daten und mit dem Bezug zu Personen. Wenn Sie in Ihrem Browser eine Internetseite aufrufen, indem Sie deren Adresse eingeben, dann muss ja in irgendeiner Form hinterlegt sein, wohin die aufgerufene Webseite „geliefert“ werden soll. Das funktioniert über die IP-Adresse, die von Ihrem Internetanbieter automatisch vergeben wird, wenn Ihr Router eine Verbindung zum Internet aufbaut.



Diese IP-Adresse ist über eine gewisse Zeit gültig und über den Anbieter Ihrem Anschluss – und damit Ihnen – zuordenbar. Die seit Jahren schwelende Diskussion um die Vorratsdatenspeicherung dreht sich genau um diesen Punkt: Wie lange muss der Bezug zwischen IP-Adresse und Anschlussinhaber gespeichert bleiben und wer hat unter welchen Bedingungen Zugriff darauf?

Onlineshopping leicht gemacht

Wenn Sie im Internet einkaufen, dann ist es viel bequemer, einmal ein Benutzerkonto beim Händler anzulegen, statt immer wieder Ihre Adresse und die Bankverbindung manuell einzugeben. Damit hinterlassen Sie natürlich schon vor dem ersten Einkauf Daten. Bei jedem Einkauf werden es mehr: Die gekauften Artikel kommen hinzu, Dinge, die Sie sich angesehen haben, und vieles mehr.

Auch das Thema Werbung ist in diesem Zusammenhang zu sehen: Haben Sie sich schon einmal darüber gewundert, dass Ihr bevorzugter Internethändler immer die richtigen Sachen im virtuellen Schaufenster hat, die fast hundertprozentig Ihren Vorlieben entsprechen? Das liegt einfach daran, dass der Händler Ihr Einkaufsverhalten kennt. Wenn Sie sich mit Ihrem Kundenkonto anmelden, dann wird eine kleine Datei, ein sogenannter Cookie, gespeichert. Damit werden Sie identifiziert, wann immer Sie die Internetseite des Shops aufrufen. Die Identifikation über den Cookie und das von Ihnen gespeicherte Einkaufsverhalten ermöglichen dann zielgerichtete Werbung.

Wenn Sie als Thriller-Fan plötzlich Kinderbücher angeboten bekommen, dann müssen Sie sich normalerweise keine Sorgen machen. Fragen Sie doch einfach in der Familie herum, wer gerade mit Ihrem PC gesurft hat. Die Wahrscheinlichkeit ist hoch, dass ein Familienmitglied hier der „Schuldige“ ist und nicht etwa ein Sicherheitsvorfall wie ein gehacktes Konto!

Ohne Ihre Daten geht es nicht

Nun haben Sie vielleicht gar kein Interesse an personalisierter Werbung und daher den Anspruch, im Internet möglichst wenige Daten zu hinterlassen. Das ist sicher kein schlechter Ansatz, doch es kann nicht bedeuten, dass Sie als Internetnutzer gar keine Daten von sich preisgeben.
Das würde schlicht nicht funktionieren, da Sie dann bestimmte Programme und Dienste nicht mehr nutzen könnten. Was bringt Ihnen ein Navigationsprogramm ohne Ihre aktuelle Position? Und wie wollen Sie etwas in einem Onlineshop bestellen, ohne ihm die Lieferadresse mitzuteilen?
Auch die viel gescholtenen sozialen Netzwerke leben ja davon, dass Sie aktuelle Lebensereignisse mit anderen Anwendern – Ihren (virtuellen) Freunden – teilen. Ohne Daten keine Freundschaften, ohne Freundschaften keine Beiträge, der Sinn eines sozialen Netzwerkes wäre dahin.

Ihre Spuren im Netz

Der Datenschatten, den Sie unweigerlich im Internet hinterlassen, hat also zwei Seiten: Auf der einen Seite ist er nahezu unvermeidbar, damit das Internet funktioniert und für Sie halbwegs komfortabel ist. Auf der anderen Seite birgt er das Risiko, dass Ihre Daten in falsche Hände gelangen und missbraucht werden.

→ Was ist ein Datenschatten?

Der Begriff des Datenschattens hat sich in den letzten Monaten immer mehr verselbstständigt. Darunter versteht man die Wolke an Daten, die jeder Anwender unweigerlich hinter sich herzieht, und das vollkommen ungewollt.

Der Prozess beginnt, wenn Sie irgendwelche Daten bei einer Webseite hinterlassen – oder auch bei einem Händler in der realen Welt. Denn Letzterer macht am Ende auch nichts anderes, als diese Daten in seinen PC einzugeben. Die Daten dienen einem bestimmten Zweck und müssen verarbeitet werden, damit die gewünschte Dienstleistung erbracht werden kann. So gelangen Ihre Daten vollkommen rechtmäßig an weitere Parteien, die dann wieder etwas damit machen.
Eigentlich – das ist eine rechtliche Anforderung des Datenschutzes – müssen Ihre Daten nach einer gewissen Zeit gelöscht werden. In vielen Fällen geschieht das aber nicht: Daten bleiben schier endlos gespeichert und sind damit dauerhaft verfügbar.
Über die Zeit kommen dann weitere Daten hinzu. Verschiedene Datenquellen werden miteinander verknüpft und durch intelligente Algorithmen verarbeitet, die Daten aus anderen Quellen anreichern und auswerten. Es dauert eine gewisse Zeit, aber dann ist Ihr Datenschatten komplett: eine fast vollständige Datenwolke Ihrer Vorlieben, Meinungen, Interessen, besuchten Orte, Freunde etc. Wer Ihren Datenschatten kennt, der kennt Sie besser als Sie sich selbst, denn Sie haben nur eine Meinung über sich. Der Datenschatten ist objektiver: Er enthält Tatsachen.

Sind Sie schon öffentlich?

Ein großer Datenschatten führt schnell dazu, dass Sie selbst nicht mehr befragt werden müssen, wenn es darum geht, eine Entscheidung für Sie zu treffen. Ob es nun um eine Kreditvergabe, ein Jobangebot oder eine personalisierte Werbung geht: Die Systeme greifen auf Ihre Daten zu und fällen eine automatisierte Entscheidung. Sie

bekommen nicht mal mit, was dann am Ende dazu führt, dass diese positiv oder negativ ausfällt.

Info

Wie viel können Daten verraten? Zu viel, wie eine junge Amerikanerin erfahren musste, als ihre bisher geheim gehaltene Schwangerschaft rüde der Familie bekannt gemacht wurde. Wie kam es dazu? Analysten der Supermarktkette Target hatten bei der Auswertung der Kaufdaten erkannt, dass der Kauf bestimmter Produkte, etwa parfümfreier Lotions oder spezieller Nahrungsergänzungsmittel, direkt mit einer Schwangerschaft in Verbindung steht. Target errechnete auf diese Weise einen „Schwangerschafts-Vorhersage-Wert“. So kam es, dass die junge Frau plötzlich Coupons für Babykleidung, Schwangerschaftskleidung und Babyausstattung zugeschickt bekam – zur Überraschung ihrer ahnungslosen Familie.

Als die Gesellschaft anfing, sich über Datenschutz und das Recht auf Privatsphäre Gedanken zu machen, war die Vision des „gläsernen Bürgers“ einer der Auslöser, von staatlicher Seite regulierend einzugreifen. Viele Jahre später zeigt sich, dass die Befürchtungen nicht unberechtigt waren. Onlineshopping, soziale Netzwerke, biometrische Sensoren in Geräten und Smartphones als Immer-dabei-Datensammler haben dazu geführt, dass Sie quasi gläsern sind, und das nur halb freiwillig.
Ganz schützen können Sie sich nicht vor einem Datenschatten. Teilweise bringt er sogar Vorteile, weil Sie objektiver bewertet werden. Der Kerngedanke des Datenschutzes ist jedoch: Sie sollen selbst entscheiden können, was andere über Sie wissen dürfen und welche

Informationen über Sie gespeichert sind. Wenn Sie aufgrund der bisherigen Ausführungen befürchten, dass Sie keine Chance haben, dies zu erreichen, dann seien Sie beruhigt: Alle Geräte, mit denen Sie arbeiten, bieten Ihnen Möglichkeiten, Einfluss darauf zu nehmen.

Der Super-GAU Datenleck

Genau diese Situation will jeder Anwender, gleich wie er das Internet nutzt, vermeiden: dass seine Daten in falsche Hände gelangen. Es ist vollkommen egal, ob es sich dabei um die Art der Bücher, die Sie lesen, oder gleich die Liste der Medikamente, die Sie bei einer Onlineapotheke bestellen, handelt. Aus all diesen Daten lassen sich mit wenig Aufwand Rückschlüsse ziehen. Je mehr Daten jemand zur Verfügung hat, desto genauer ist das Bild, das er von Ihnen zeichnen kann. Und je genauer er Sie kennt, desto besser kann er Ihr Verhalten vorhersagen und Ihnen Dinge vorgaukeln, die Sie gerne glauben wollen.
Noch schlimmer: Kommen Angreifer an Ihre Daten, dann können sie im schlimmsten Fall sogar Ihre Identität übernehmen, also im Internet so agieren, als seien sie Sie. Das führt dann nicht nur zu einem Reputationsschaden, sondern kann auch immense finanzielle Schäden mit sich bringen. Bestellungen, die mit Ihrem Kundenkonto und damit Ihren Zahlungsdaten getätigt und an eine fremde Adresse geliefert werden, abstruse Meinungen, die in Ihrem Namen geäußert werden und vieles mehr. Das sind nicht nur Schreckgespenster, sondern so etwas kommt immer wieder vor.
Es ist unmöglich, alle ernst zu nehmenden Hacks aufzulisten, die bisher stattgefunden haben. Hier finden Sie einige derer, die besonders viel Aufsehen erregt haben.

Info

Sind Sie betroffen? In regelmäßigen Abständen gibt es Nachrichten über gehackte Benutzerkonten, frei im Internet auffindbare persönliche Daten oder Angriffe auf Netzwerke. Es lässt sich nicht mit Sicherheit sagen, ob Sie schon einmal betroffen waren. Sie können aber unter der Adresse https://haveibeenpwned.com/ nachsehen, ob Ihre E-Mail-Adresse (die in den meisten Fällen gleichzeitig Ihr Benutzername bei der Anmeldung auf einer Webseite ist) schon einmal in einer im Internet zum Kauf angebotenen Datenbank gefunden wurde. Falls ja, sollten Sie schnellstmöglich Ihr Passwort ändern. Die Webseite wird regelmäßig erweitert, wenn es ein neues größeres Datenleck gab.

Collection #1

Collection #1 war eigentlich kein eigenes Datenleck, sondern eine Kombination von vielen. Die Datenbank, die im Januar 2019 im Internet gefunden wurde, enthielt 2,7 Milliarden Einträge mit 773 Millionen E-Mail-Adressen und zugehöriger Passwörter. Offensichtlich waren hier Datenbanken aus anderen Hacks mit neuen Datensätzen zusammengemischt und dann als eine große Datenbank verkauft worden. Wenn Sie die Kombination aus E-Mail-Adresse und Passwort häufiger nutzen (was keine gute Idee ist!), dann haben Sie eine gute Chance, dass jemand einfach mal versucht, diese Kombination bei allen möglichen Shops auszuprobieren und bei Erfolg davon Gebrauch zu machen.

PlayStation Network

Was kann an einem Benutzerkonto einer Spielekonsole gefährlich sein? Nun, zum einen bestehen die Zugangsdaten auch hier aus E-Mail-Adresse und Passwort, zum anderen können im Konto richtige Werte liegen: Spieler sammeln über die Jahre Auszeichnungen, Ausrüstungsgegenstände, Reputation in der Spielewelt. Und sie hinterlegen eine echte oder virtuelle Währung, um Software, Erweiterungen oder Ausrüstung für die Konsole oder die Spiele zu kaufen. Ist das Konto gehackt – was bei Sonys PlayStation Network leider schon mehrfach vorgekommen ist –, dann ist all das in Gefahr.

Der Hilton-Hack

Angriffe müssen nicht einmal virtuell stattfinden. Die Hotelkette Hilton musste 2015 eingestehen, dass in Geschenkeshops mehrerer Hotels der Gruppe betrügerische Transaktionen aufgefallen waren. Hacker hatten nämlich die (elektronischen) Kassensysteme der

Shops kompromittiert und darüber Mengen an vermeintlichen Käufen laufen lassen. Die Betroffenen konnten zwar in den meisten Fällen nachweisen, dass sie nicht die Verursacher waren, für Kreditkartenunternehmen und Shops war es aber eine bittere Erfahrung.

Der Mastercard-Hack

Kreditkartenunternehmen sind ein beliebtes Ziel von Hackern. Die Kombination aus Kreditkartennummer, Sicherheitscode und Name des Karteninhabers bietet schnellen Erfolg: Ist die Transaktion auf die Kreditkarte einmal freigegeben, dann sind Geld oder bestellte Ware kaum noch aufzuhalten. Diese Erfahrung musste Mastercard im August 2019 gleich doppelt machen: Erst fanden sich im Internet die Daten Zehntausender Kunden des Bonusprogramms „Priceless Specials“ mit Vor- und Nachname, Geburtsdatum, E-Mail-Adresse und teilweise auch Postanschrift und Handynummer. Zusätzlich waren darin bis auf wenige Ziffern unkenntlich gemachte Kreditkartennummern enthalten. Einige Tage später fand sich eine vom Umfang her nahezu identische Datei mit kompletten Kreditkartennummern im Netz. Viele Betroffene tauchten in beiden Dateien auf. Auch wenn die Sicherheitscodes fehlten, die für einen unmittelbaren Missbrauch nötig gewesen wären, war das ein Schock für die Betroffenen.

Vodafone und die Kundendaten

Mobilfunkanbieter haben eine Menge Kundendaten gespeichert. Normalerweise liegen diese sicher in Datenbanken. Es sei denn, jemand kopiert sie sich. So geschehen im Jahr 2013, als die Daten von zwei Millionen Vodafone-Kunden gestohlen wurden. Offensichtlich durch einen Insider, der sich Zugang zu den Datenbanken

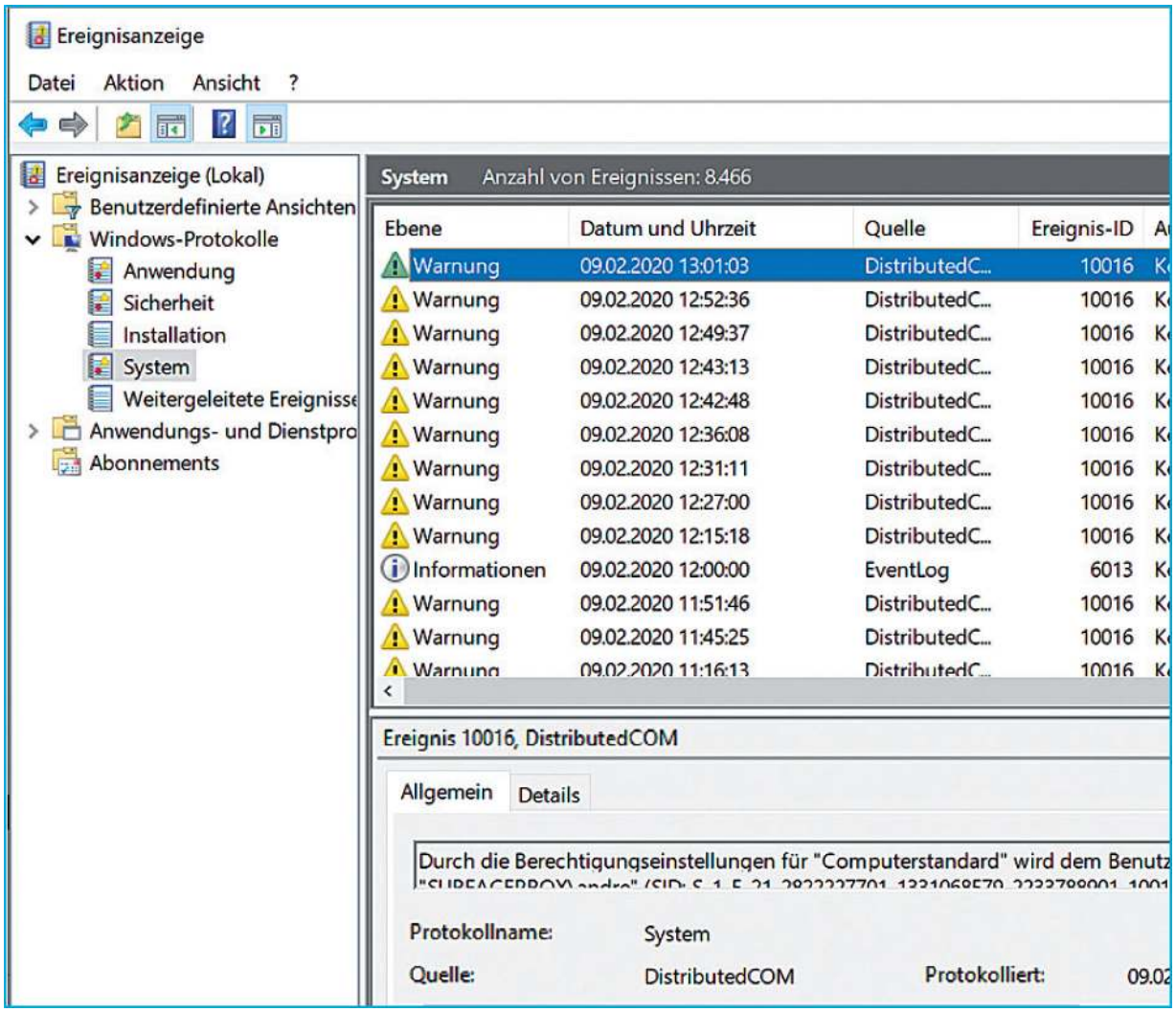
verschafft hatte. Zu den gestohlenen Daten gehörten Name und Vorname, das Geburtsdatum, das Geschlecht, die Bankleitzahl und die Kontonummer. Vodafone schrieb alle Betroffenen an und versuchte zu beruhigen: Es sei nach Angaben unabhängiger Sicherheitsexperten nicht möglich, mit den gestohlenen Daten direkt auf Bankkonten zuzugreifen. Nun, direkt vielleicht nicht. Allerdings sind Bankverbindung, Geburtsdatum und Adresse meist die Daten, die zur Absicherung bei einer telefonischen Anfrage bei Versicherungen und Banken abgefragt werden.

Wo sind Ihre Daten?

Daten von sich preiszugeben, erscheint risikoreich. Doch es geht nicht anders. Ohne Adresse kein Versand von Ware, ohne Kontoverbindung keine Zahlung, ohne Suchmaschine keine Suchergebnisse. Sie werden es nicht schaffen, das Internet komplett anonym zu nutzen, aber es hilft schon mal zu wissen, wo überhaupt welche Daten vorhanden sind und wer diese Daten sammelt. Denn dann können Sie bewusster mit Ihren Daten umgehen.

Protokolldateien und Telemetrie

Einer der größten Datenspeicher, den Sie benutzen, sind Ihre technischen Geräte. Der PC oder Mac, das Tablet, diese Geräte nutzen Sie für alle erdenklichen Tätigkeiten. Ob Sie einfach nur in Windows herumnavigieren oder in einem Programm Daten eingeben, automatisch werden Protokolle erzeugt, Dateien abgelegt und Elemente zwischengespeichert. Die meisten Daten sind notwendig und in den richtigen Händen vollkommen unkritisch.



Ein Betriebssystem wie Windows oder macOS ist ein komplexes System, in dem viele Komponenten ineinandergreifen. Das, was Sie sehen, also die Apps und die Benutzeroberfläche, ist nur die Spitze des Eisbergs. Der Anbieter sammelt eine Menge von Daten, aber nicht, um Sie auszuspionieren, sondern um ein einwandfrei laufendes System sicherzustellen. Egal, was Sie tun, es wird standardmäßig aufgezeichnet und ausgewertet.
Die Ereignisanzeige beispielsweise gibt Ihnen einen guten Überblick, was im System passiert ist. Anmeldeversuche, Fehler in den Geräten und Apps, Abstürze, Freigaben von Ressourcen und vieles mehr können Sie darin sehen und

damit einen Eindruck bekommen, was das Betriebssystem so alles mitschreibt.
Auch die Telemetriedaten sind eine riesige Quelle an Informationen. Dabei handelt es sich um Messwerte, die an den Anbieter übermittelt werden: Abstürze, besondere Ereignisse, Auslastung von Prozessor und Speicher und vieles mehr. Microsoft sieht Windows nicht nur als einzelnes Betriebssystem, sondern als Ökosystem. Es gibt viel zu viele Komponenten, viel zu viele Apps und Benutzereinstellungen, als dass man alle möglichen Kombinationen testen könnte. Daher nutzt Microsoft die Daten der Nutzer.

Daten sammeln für mehr Sicherheit

Alle möglichen Informationen werden anonymisiert an die Microsoft-Server weitergeleitet. Treten bestimmte Fehlersituationen wiederholt und bei verschiedenen Anwendern auf, dann wird dies erkannt. Hier hat die Datensammlung einen positiven Effekt: Anhand der Auswertungen können Fehler entdeckt und in einem der folgenden Updates behoben werden. Davon profitieren alle Anwender.

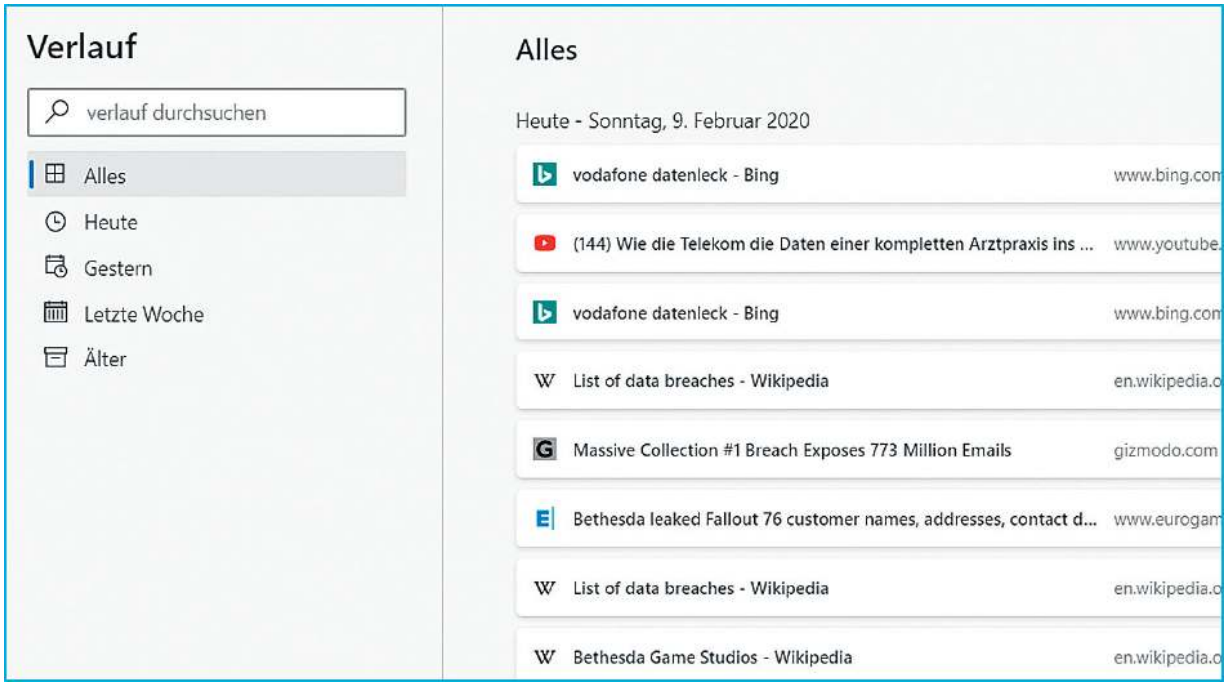
Die Benutzerdaten

Auf einem PC wie auch auf einem Mac können sich mehr als ein Benutzer anmelden. Zu einem Benutzer gehören dann immer bestimmte Verzeichnisse, die die Dokumente, die Videos, die Bilder und auch Einstellungen und andere Dateien enthalten. Auch wenn diese Dateien immer nur für den jeweils berechtigten Benutzer zugänglich sind und kein anderer Benutzer darauf zugreifen kann, sind sie trotzdem auf dem Gerät gespeichert.
Wenn Sie an einem Computer in einem Firmennetzwerk arbeiten, finden sich diese Profile nicht nur lokal auf Ihrem

Rechner, sondern auch auf einem zentralen Server. Bei jeder Anmeldung werden automatisch die Benutzerdaten vom Server heruntergeladen und lokal gespeichert.

Die Historie Ihrer Sitzungen

Wenn Sie mit Windows oder macOS arbeiten, führen Sie bestimmte Schritte immer wieder aus. Ob Sie nun eine Datei öffnen und diese später weiterbearbeiten oder eine Webseite aufrufen und später wiederfinden möchten: Die Betriebssysteme sammeln diese Informationen und stellen Sie Ihnen dann wieder zur Verfügung. Die Historie der geöffneten Dateien in den Office-Programmen, die Liste der geöffneten Webseiten, Suchvorschläge in Bing, all diese Informationen sind ungemein hilfreich. Allerdings sind sie auch mit Risiken verbunden. Vielleicht wollen Sie zum Beispiel nicht, dass ein Kollege sieht, dass Sie mehrfach ein bekanntes Jobportal im Internet aufgerufen haben.



Die Analyse Ihrer Eingaben

Auch bei Ihren Eingaben versucht das Betriebssystem Sie zu unterstützen. Windows und macOS korrigieren Texte, die Sie eingeben, automatisch. Wenn Sie aber bestimmte Begriffe verwenden, die im Standard nicht bekannt sind, werden diese immer wieder falsch korrigiert oder als Fehler angezeigt. Nichts ist einfacher, als diese Begriffe dann in Ihr Benutzerwörterbuch aufzunehmen, damit sie nicht mehr als Fehler angezeigt werden. Dieses Benutzerwörterbuch ist ein Quell an Informationen für jeden, der darauf zugreifen kann. Nirgendwo sonst findet man konzentrierter Hinweise darauf, mit welchen Themen Sie sich beschäftigen.
Dasselbe gilt für die Umsetzung von Sprache und Schrift: Wenn Sie ein Gerät mit einem Stift haben, dann können Sie nicht nur über die Tastatur Text eingeben, sondern auch handschriftlich. Nun ist die Schrift eines jeden Anwenders einzigartig. Das Betriebssystem hat am Anfang einiges zu tun, um Ihre Schrift zu erkennen. Erst mit der Zeit – und vor allem durch die Korrekturen, die Sie vornehmen – wird die Erkennung besser. Das funktioniert daher so gut, weil Ihr Computer die Schriftdaten und die Korrekturen zur Analyse einsendet. Die Rechenkapazität Ihres lokalen Geräts reicht dafür bei Weitem nicht aus.

Cortana oder Siri als Sprachassistenten auf Ihrem PC oder Mac und zusätzlich installierte wie Amazons Alexa sind ähnlich aufgestellt: Sie nehmen über das Mikrofon Ihre Stimme auf, schicken sie an den Server des Anbieters und bekommen den erkannten Befehl zurückübermittelt. Einfache Befehle wie „Alexa, schalte Fernseher ein“ sind sicher unkritischer als Text, den Sie über die Spracherkennung eingeben. Denn dieser enthält jedes einzelne Zeichen Ihrer Äußerung. Hier kollidiert der Wunsch nach komfortablem Arbeiten mit dem Anspruch, dass möglichst wenige Daten außerhalb der eigenen Zugriffsmöglichkeiten gespeichert sind.

Der Internetbrowser

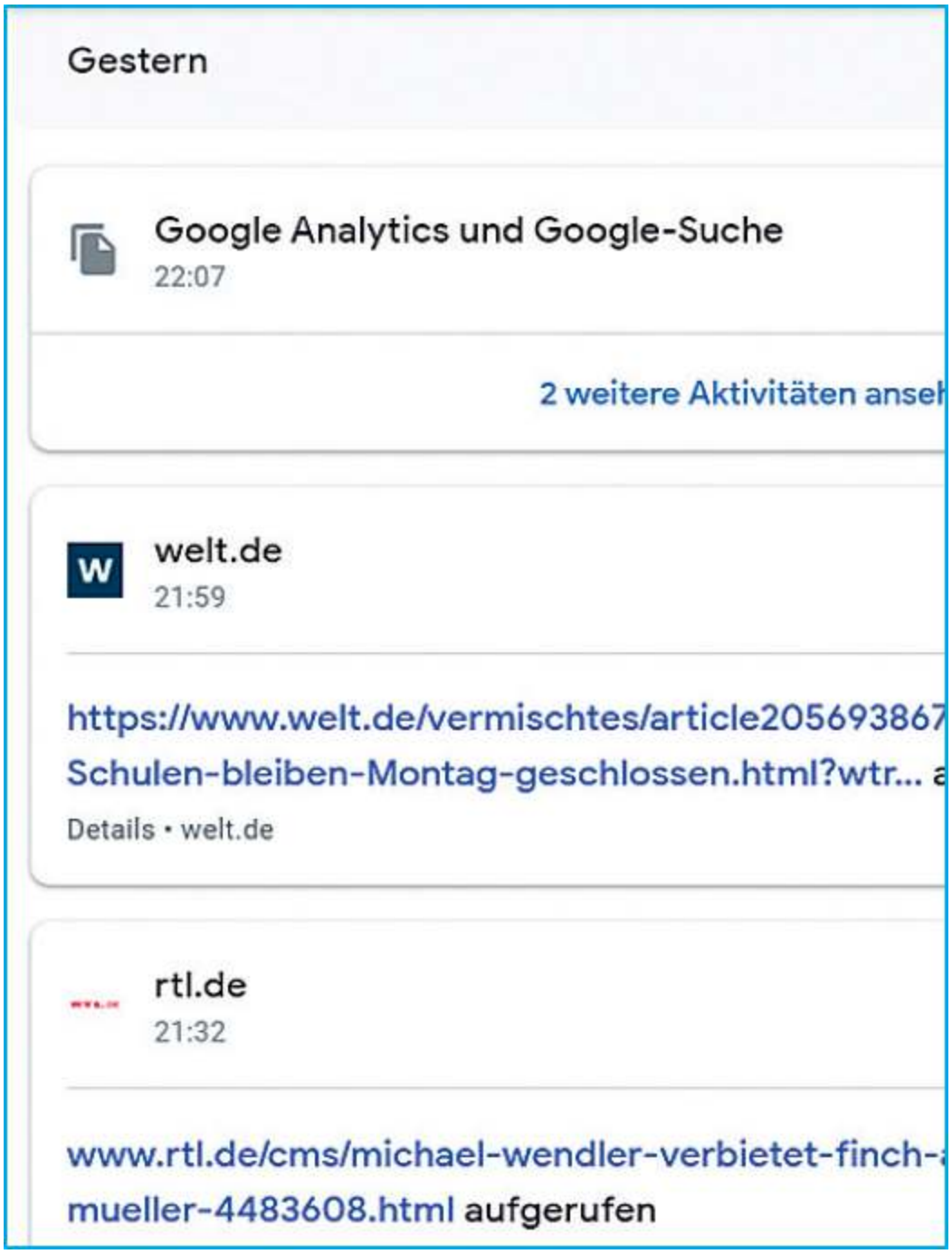
Während die automatisch aufgezeichneten Informationen, die das Betriebssystem verwaltet, meist auf Ihrem Rechner verbleiben, verhält es sich beim Surfen im Internet ein wenig anders. Hier werden die Informationen an einen Rechner außerhalb Ihres eigenen Netzwerkes übertragen.

Was dort mit ihnen geschieht, liegt meist nicht in Ihrer Kontrolle. Auf jeden Fall übermitteln Sie Ihre eigene IP-Adresse ins Internet, die zum Übertragen der abgerufenen Daten aus dem Internet auf Ihren Rechner unbedingt benötigt wird. Wie schon erwähnt, verwenden darüber hinaus viele Internetseiten Cookies, um Sie bei einem erneuten Besuch zu identifizieren und Ihnen passende Informationen und zielgerichtete Werbung zu zeigen.

→ Keine Angst vor Cookies!

Lassen Sie sich nicht verunsichern: Ein Cookie ist kein Programm und kein Virus, sondern lediglich eine kleine Textdatei, die der Webseite die Identifikation des Besuchers ermöglicht. Anrichten kann ein Cookie für sich allein auf Ihrem Rechner erst einmal gar nichts. Außerdem gibt es Möglichkeiten, Cookies loszuwerden oder gar nicht erst zu speichern, wie Sie ab S. 104 erfahren.

Wann immer Sie eine Webseite aus dem Internet abrufen, werden deren Elemente automatisch auf Ihrer Festplatte gespeichert. Eine Webseite besteht aus Bildern, aus kleinen Programmteilen, aus Text und anderen Komponenten. Ihr Internetbrowser setzt die Seite dann aus diesen Elementen zusammen und zeigt sie Ihnen auf dem Bildschirm an. Diese temporären Dateien bleiben so lange auf Ihrer Festplatte, bis sie automatisch gelöscht werden oder Sie den Löschvorgang manuell starten. Ebenfalls speichert Ihr Browser die Liste der aufgerufenen Webseiten, Daten, die Sie in Formulare eingeben, und gegebenenfalls sogar Benutzernamen und Passwörter.



Schließlich gibt es ein eigenes Verzeichnis auf der Festplatte, in dem alle Dateien, die Sie aus dem Internet heruntergeladen haben, gespeichert sind. Auf diese Dateien können Sie wieder zugreifen, wenn Sie ein Programm oder eine Datei erneut verwenden wollen. Das

ist vollkommen unabhängig davon, welchen Browser oder welches Betriebssystem Sie verwenden.

E-Mails

Wenn Sie per E-Mail kommunizieren, dann schicken Sie nicht nur Textinhalte an bestimmte E-Mail-Adressen, sondern Sie hängen den E-Mails oft auch Dateien an. All diese Elemente werden nicht nur auf dem E-Mail-Server gespeichert, sondern auch auf Ihrem PC im E-Mail-Programm.
Was dabei oft übersehen wird: Eine erhaltene E-Mail ist oft nur der Anfang einer ganzen Reihe. Sie bekommen eine E-Mail, beantworten sie, erhalten daraufhin wieder eine Antwort und so geht es immer weiter. Die E-Mails legen Sie dann in einem Ordner auf der Festplatte ab. In der Summe kann eine einzelne E-Mail nachher an vielen verschiedenen Orten liegen, was das Löschen zu einer Herausforderung macht.
Auch bei E-Mails gibt es eine Vielzahl von Protokollinformationen: Nach dem Versand hält Ihr Computer in Zusammenarbeit mit dem E-Mail-Server akribisch fest, über welche Server die E-Mail läuft, zu welcher Zeit und mit welcher IP-Adresse sie versandt wurde und vieles mehr. Es ist kaum möglich, eine E-Mail ohne spezielle Maßnahmen anonym zu verschicken!

Dateien auf dem Rechner und in der Cloud

Der eigentliche Schatz, den Sie auf Ihrem Rechner verwalten, sind die Dateien. Sie installieren Programme, geben dort Daten ein und speichern das Ergebnis als Datei auf der Festplatte ab. Diese Dateien enthalten eine riesige Menge an Informationen – nicht nur die, die Sie selbst eingegeben haben, sondern auch viele

Verwaltungsinformationen, die automatisch vom Betriebssystem und den Programmen hinzugefügt werden. Mit den neuen Windows- und Office-Versionen hat ein weiterer Speicherort Einzug auf Ihrem PC gehalten: die Cloud. Dokumente werden nicht nur lokal gespeichert, sondern auch an einem Speicherort, der irgendwo im Internet liegt. Das geschieht in vielen Fällen sogar automatisch. Natürlich sind die Daten in der Cloud geschützt, oft sogar besser als auf Ihrem lokalen PC. Denn für die Sicherheit Ihrer Daten ist dann der Cloudanbieter, zum Beispiel Microsoft, verantwortlich. Dennoch ändert das nichts daran, dass Daten, die nicht auf Ihrem PC liegen, potenziell der Gefahr von Angriffen aus dem Internet ausgesetzt sind.

Info

Faktor (Un-)Ordnung: So sehr Sie sich vornehmen, Ihre Dateien strukturiert in die richtigen Ordner zu speichern, es kommt immer wieder vor, dass eine Datei versehentlich in einem beliebigen anderen Ordner abgelegt wird. Diese Dateien dann später zu finden und gegebenenfalls auch zu löschen, ist eine echte Herausforderung!

Soziale Netzwerke: Daten als Währung

Es ist fast unmöglich, sich ganz von sozialen Netzwerken fernzuhalten. Wer auf „Welches Twitter-Handle hast du denn?“ oder „Lass mal auf Xing netzwerken!“ nur antworten kann, dass er auf den Plattformen nicht vertreten ist, erntet schnell irritierte Blicke. Außerdem entgehen einem so viele Kontaktmöglichkeiten. Man mag zu Facebook stehen, wie man will: Wie sonst halten Sie